

# 湖北工业职业技术学院网络与信息系统安全管理办法

(2019年第10次院长办公会及2019年第13次党委会通过)

**第一条** 为了加强信息安全保障能力，建立健全安全管理体系，提高整体的网络与信息安全水平，保证网络与信息系统安全稳定运行，根据国家相关法律和有关规定，结合我校实际，制定本办法。

**第二条** 学校任何单位及个人均应按照国家有关法律法规要求，合法使用校园网络及信息系统资源，不得有危害校园网络、信息系统以及利用校园网络、信息系统侵犯国家、集体和个人合法权益的行为，不得从事违法犯罪活动和以营利为目的的商业活动。

**第三条** 网络与信息系统安全必须贯穿学校信息化建设始终，做到“同步规划、同步建设和同步管理”。

**第四条** 学校网信办负责学校网络与信息系统安全管理，负责制定学校网络与信息系统安全管理制度及安全应急预案，负责学校网络与信息系统安全事件的应急处置工作。

**第五条** 各单位制定本单位信息系统安全管理细则及安全应急预案，负责本单位信息系统安全事件应急处置工作。

**第六条** 网络与信息系统安全事件包括：

1. 网络攻击事件（校园网络与信息系统因病毒感染、非法入侵等造成学校网站页面被恶意篡改，信息系统数据被篡改、删除、泄露等）；

2. 设备故障事件（校园网络与信息系统因设备故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等）；

3. 信息内容安全事件（利用校园网络在校内外传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公共利益等）；

4. 灾害性事件（因洪水、火灾、雷击、地震、非正常停电等外力因素导致网络与信息系统损毁，造成业务中断、系统宕机、网络瘫痪）。

**第七条** 凡出现网络与信息系统安全事件，各单位及用户应在第一时间向网信办报告，启动应急预案，并按照相应预案进行应急处置。

**第八条** 应急处置工作结束后，责任单位向网信办和上级部门提交事件调查处置报告。必要时，网信办组织专家进行核查，督促消除安全隐患。

**第九条** 为应对网络与信息系统安全紧急事件，应预留一定的安全冗余设备。重要信息系统均应建立备份系统，保证重要数据在受到破坏后可紧急恢复。

**第十条** 学校成立网络信息安全应急处置队伍，提供技术支持与应急支援。各单

位应指定专人负责本单位网络与信息系统的紧急事件应急处置工作。

**第十一条** 学校每年至少安排一次演练，各单位每年至少安排一次内部应急演练，不断完善应急办法，提高应急处置能力。

**第十二条** 各单位应当切实履行网络与信息系统的保护职责，加强安全管理，主动开展安全防护工作。对于玩忽职守、疏于管理、造成网络与信息系统安全事件的单位，主要负责人要承担领导责任。

**第十三条** 对于校园网络与信息系统违法行为及涉嫌侵害国家信息安全的犯罪行为，依照有关法律法规处理。

**第十四条** 《学校网络与信息系统安全应急预案》《学校服务器（信息系统）托管服务管理办法》《学校数据中心虚拟主机管理办法》及网络与信息安全相关制度、办法和实施细则由学校图文信息中心（网信办）在本办法基础上依法依规制订执行。

**第十五条** 本办法由学校网信办负责解释，自发布之日起实施。